UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/769,038 | 01/30/2004 | Daniel M. Bodorin | MS307659.01/MSFTP2452US | 7942 |

27195 7590 03/05/2009

AMIN, TUROCY & CALVIN, LLP
127 Public Square
57th Floor, Key Tower
CLEVELAND, OH 44114

| EXAMINER | |
|---|---|
| ARMOUCHE, HADI S | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2432 | |

| NOTIFICATION DATE | DELIVERY MODE |
|---|---|
| 03/05/2009 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docket1@thepatentattorneys.com
hholmes@thepatentattorneys.com
lpasterchek@thepatentattorneys.com

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/769,038 | BODORIN ET AL. | |
| | Examiner | Art Unit | |
| | HADI ARMOUCHE | 2432 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *24 November 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01/30/2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

1. This communication is in response to applicant's amendment filed on 11/24/2008. Claims 1-4 have been amended, claims 17-20 have been added. Claims 1-20 remain pending.

### *Response to Arguments*

2. Applicant's arguments filed on 11/24/2008 have been fully considered but they are not persuasive.

3. It has been argued (pages 9-11 of the remarks) that White does not teach the newly amended limitation. Namely, the Workflow Supervisor sends the sample to a separate workload machine/system to perform a classification task to determine the code module's type.

Applicant's interpretation of the reference is noted. However, White in page 25 under "Macro Viruses" section first paragraph teaches analyzing the type of the code module wherein the type is the format and the language. Moreover, White in page 23 under "Scaling the Analysis center" section first paragraph teaches that all the operations in the system are running in parallel. An ordinary skill in the art knows that a system can comprise of different sub-systems to do the function of the current claimed invention especially that the claim states: "A ...system.....comprising" (open ended) and not "consisting". Moreover, the applicant in the specification page 9 lines 24-25 states: "*Examining a code module 212 and determining the type of code module is known in the art.*"

4. Applicant's arguments with respect to claims 1-4 that White does not teach the newly amended limitation have been considered but are moot in view of the new ground of rejection. Namely, the limitation that the malware detection system is configured to report whether the code module is malware based at least in part of the degree that the code module's exhibited execution behaviors match the exhibited behaviors of a known malware.

***Claim Rejections - 35 USC § 103***

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over White et al. ("Anatomy of a Commercial-Grade Immune System", http://citeseer.ist.psu.edu/white99anatomy.html, 1999), hereafter "White" in view of Schultz et al. (US 2003/0065926) referred to hereinafter by Schultz.

7. Regarding claim 1, White discloses a malware detection system and means for determining whether a code module is malware according to the code module's exhibited behaviors (Fig. 3, page 14), the system comprising:

at least one dynamic behavior evaluation module (Fig. 6, page 20, Analysis Center reads on dynamic behavior evaluation module), wherein each dynamic behavior evaluation module provides a virtual environment for executing a code module of a particular type (Section "Creation of the replication environment", Page

20: paragraph 1: lines 1-5), and wherein each dynamic behavior evaluation module records some execution behaviors of the code module as it is executed, wherein the execution behaviors of the code module are recorded into a behavior signature corresponding to the code module: (Fig. 6, page 20: item "archive" and Section "Analysis", page 21: paragraph 1: lines 5-6, extract good signature and stores in the archive for developing virus definition reads on each dynamic behavior evaluation module records some behaviors which may be exhibited by the code module as it is executed into a behavior signature);

a management module, wherein the management module obtains the code module, and wherein the management module evaluates the code module to determine the code module's type (page 23 under "Scaling the analysis center" 1st paragraph and page 25 under "Macro Viruses: 1st paragraph) , and wherein the management module selects a dynamic behavior evaluation module to execute the code module according to the code module's type (Fig. 6: page 20: item "workflow supervisor" and Section "Macro Viruses": page 25: paragraph 1: lines 5-7, supervisor accept suspected virus sample and feed into different virtual environment for each format and language of Macro Virus reads on a management module for obtaining the code module and selecting a dynamic behavior evaluation module to execute the code module according to the code module's type);

a malware behavior signature store storing at least one known malware behavior signature of a known malware (Fig. 3: item archive, Page 20, and Section "The Supervisor" pages 18 and 19, paragraph 3: lines 1-2 and Section "Definition

generation", Page 21: paragraph 1: lines 1-10, archive and virus definition file reads on malware behavior signature store storing at least one known malware behavior signature);

a behavior signature comparison module that obtains the behavior signature of the code module and compares the behavior signature of the code module to the known malware behavior signatures in the malware behavior signature store to determine whether the exhibited execution behaviors of the code module match the exhibited execution behaviors of a known malware (Section "An active network to Handle Epidemics and Floods – Over view", pages 13-15: paragraph 5: lines 1-2, gateway scans the sample file against the latest virus definition reads on a behavior signature comparison module that obtains the behavior signature and compares the behavior signature to the known malware behavior signatures in the malware behavior signature store to determine whether the exhibited behaviors of the code module match the exhibited behaviors of known malware); and

Even though White teaches that the malware detection system is configured to report whether the code module is malware or not (Section "An active network to Handle Epidemics and Floods – Over view", pages 13-15), White does not explicitly teaches that the malware detection system is configured to report whether the code module is malware based at least in part of the degree that the code module's exhibited execution behaviors match the exhibited behaviors of a known malware.

Schultz teaches that the malware detection system is configured to report whether the code module (executable) is malware based at least in part of the

degree (probability or likelihood) that the code module's exhibited execution behaviors match the exhibited behaviors of a known malware [abstract last 8 lines and paragraph 0022].

At the time of the invention was made, it would have been obvious to an ordinary skill in the art to combine Schultz's teachings in White's system. The motivation/suggestion would have been to make the system for reliable and secure by detecting malicious executables [Schultz, paragraph 0005].

8. The system of claim 2, the method of claim 3 and the computer-readable medium of claim 4 have the same limitations as claim 1 and hence same rejection rational is applied.

9. For claim 5 and similar claims 8, 11 and 14, White discloses wherein recording some execution behaviors of the code module as it is executed comprises recording executed behaviors that are identified in a predefined set of execution behaviors to record (page 21, paragraph 5: virus definition...set of source files...virus analysis).

10. For claim 6 and similar claims 9, 12, and 15, White discloses wherein the predefined set of execution behaviors to record corresponds to the dynamic behavior evaluation module in which a code module of a particular type may be executed. (Fig. 3: page 20: item "workflow supervisor" and Section "Macro Viruses": page 25: paragraph 1: lines 5-7, supervisor accept suspected virus sample and feed into different virtual environment for each format and language of Macro Virus reads on a management module for obtaining the code module and selecting a dynamic behavior evaluation module to execute the code module according to the code module's type; page 19,

paragraph 3 and paragraph 5: virus definition version…superset of previous definition…; page 20, paragraph 1 "classification"...determine type...)

11. For claim 7 and similar claims 10, 13 and 16, White discloses wherein the predefined set of execution behaviors to record corresponds to a set of system calls (page 20, paragraph 1 “classification”.

12. For claim 17 and similar claim 18, White discloses wherein the malware detection system is further configured to report a positive identification of a known malware (Section "An active network to Handle Epidemics and Floods – Over view", pages 13-15: paragraph 5: lines 1-2, gateway scans the sample file against the latest virus definition reads on a behavior signature comparison module that obtains the behavior signature and compares the behavior signature to the known malware behavior signatures in the malware behavior signature store to determine whether the exhibited behaviors of the code module match the exhibited behaviors of known malware).

13. For claims 19 and similar claim 20, Schultz teaches whether the code module (executable) is malware based at least in part of the degree (probability or likelihood) that the code module’s exhibited execution behaviors match the exhibited behaviors of a known malware comprises reporting a positive identification of a known malware [abstract last 8 lines and paragraph 0022].

## *Conclusion*

14. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to HADI ARMOUCHE whose telephone number is (571)270-3618. The examiner can normally be reached on M-Th 7:30-5:00 and Fridays half day.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/H. A./
HADI ARMOUCHE
Examiner, Art Unit 2432
02/25/2009

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432